



SharkFest '18 Europe



Crash Course: IPv6 & Network Protocols

by looking at packets!

Johannes Weber

Network Security Consultant



#whoami: Johannes Weber



- Network Security Consultant
@ TÜV Rheinland i-sec GmbH
 - (Next-Gen) Firewalls
 - VPN/Crypto
 - Routing/Switching
- IPv6, DNS, NTP
- <https://weberblog.net>
- [@webernetz](#)





Agenda/Motivation



- Many „unknown“ packets
 - IPv6
 - Network Protocols
- Crash course -> fast, no deep dive & skipping ;)
- Normally: 2 day workshop for IPv6 only
- Never ending acronyms

- Who is familiar with IPv6?



Tracefiles



- <https://tinyurl.com/ipv6-crash-course>
- -> download of „weber01.zip“
- -> 3x pcaps
- Plz do me a favour: listen first ;)
- flavoured with 12x challenges







IPv6



- IPv4 space is exhausted
- IPv6 brings enough addresses ;)
 - every client is global addressable
 - end-to-end communication (no NAT!)
 - subnets for everyone
- Only layer 3 changes (almost)
- No broadcast anymore, but multicast



IPv6 Addresses



- 128 bits long, hexadecimal, 8 groups called „hextets“
- Notation: address/prefix-length
- Address abbreviation
 - `2001:0db8:0000:0000:cafe:0000:1200:f1b2`
 - `2001:db8::cafe:0:1200:f1b2`
- Subnets ALWAYS /64



IPv6 Addresses



- Unspecified `::`
- Link-Local, LL `fe80::`
- Multicast `ff00::/8`, mostly `ff02::`

- Every (!) node gets one link-local
AND couple of global unicast addresses, GUA



IPv6 Address Assignment



- Manual, stateful DHCPv6
- SLAAC through router advertisement, RA
 - Router sends RA with /64 prefix
 - Client generates interface-ID, IID
 - Client sends duplicate address detection, DAD through neighbor solicitation, NS
 - Recursive DNS server through RA or stateless DHCPv6



IPv6 Address Assignment



- IIDs normally through EUI-64, i.e., MAC address
::ca0e:14**ff:fe**7e:339f
- or stable opaque
::263d:a07f:df5:bcfb
- and/or temporary (privacy extension, PE)



IPv6 Address Assignment



- Problem: Everything is within ICMPv6
- Suite called Neighbor Discovery Protocol, NDP
 - Router Solicit./Advert.: `icmpv6.type == 133/134`
 - Neighbor Solicit./Advert.: `icmpv6.type == 135/136`
- DHCPv6: `dhcpv6`
- Use Coloring Rules for RS/RA, NS/NA, DAD



IPv6 Address Assignment



Wireshark · Coloring Rules Default

Name	Filter
<input checked="" type="checkbox"/> ICMPv6 DAD	<code>icmpv6.type == 135 && ipv6.src == ::</code>
<input checked="" type="checkbox"/> ICMPv6 NS/NA	<code>icmpv6.type == 135 icmpv6.type == 136</code>
<input checked="" type="checkbox"/> ICMPv6 RS/RA	<code>icmpv6.type == 133 icmpv6.type == 134</code>
<input checked="" type="checkbox"/> Bad TCP	<code>tcp.analysis.flags && !tcp.analysis.window_update</code>
<input checked="" type="checkbox"/> HSRP State Change	<code>hsrp.state != 8 && hsrp.state != 16</code>
<input checked="" type="checkbox"/> Spanning Tree Topology Change	<code>stp.type == 0x80</code>
<input checked="" type="checkbox"/> OSPF State Change	<code>ospf.msg != 1</code>



IPv6 Address Assignment



CCNP-SWITCH-final.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

lcmpv6

No.	Time	Time Delta	Source	Destination	VLAN	Src Port	Dst Port	Protocol
239	21.047809	0.086510	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
248	21.055761	0.000498	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
364	26.993950	0.017394	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
365	26.998683	0.004733	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
600	52.303124	0.027765	fe80::21e:7aff:fe79:3f11	ff02::1	10		ICMPv6	
607	52.985973	0.058760	fe80::5:73ff:fea0:7f	ff02::1	121		ICMPv6	
849	81.047578	0.203531	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
855	81.056339	0.000511	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
937	86.995261	0.380315	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
938	86.999513	0.004252	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
1145	109.687776	0.030748	fe80::21e:7aff:fe79:3f11	ff02::1	121		ICMPv6	
1179	113.984200	0.304294	::	ff02::1:ffe9:bb47	30		ICMPv6	
1187	114.992853	0.105264	fe80::221:70ff:fee9:bb47	ff02::2	30		ICMPv6	
1220	118.781064	0.036130	fe80::221:70ff:fee9:bb47	ff02::2	30		ICMPv6	
1267	122.778808	0.003000	fe80::221:70ff:fee9:bb47	ff02::2	30		ICMPv6	
1425	141.048399	0.153152	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
1431	141.056900	0.001504	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
1512	146.996573	0.061511	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
1513	147.000321	0.003748	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
1975	195.984811	0.111397	fe80::21e:7aff:fe79:3f11	fe80::214:69ff:fe9e:1141	121		ICMPv6	
1976	195.989181	0.004370	fe80::214:69ff:fe9e:1141	fe80::21e:7aff:fe79:3f11	121		ICMPv6	
1977	195.989437	0.000256	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
1978	195.992932	0.003495	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
2020	200.929447	0.025754	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2021	201.049222	0.119775	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
2027	201.057715	0.001624	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
2031	201.069218	0.000248	fe80::214:69ff:fe9e:1141	fe80::21e:7aff:fe79:3f11	121		ICMPv6	
2032	201.072968	0.003750	fe80::21e:7aff:fe79:3f11	fe80::214:69ff:fe9e:1141	121		ICMPv6	
2072	202.033377	0.123018	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2079	203.125304	0.208297	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2097	204.933320	0.003119	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2098	205.129356	0.196036	fe80::5:73ff:fea0:7f	ff02::1	121		ICMPv6	
2111	205.965231	0.023754	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2117	206.997891	0.050376	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2136	208.937445	0.267796	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2151	210.029363	0.059761	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2162	211.121533	0.068257	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	

CCNP-SWITCH-final.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

lcmpv6

No.	Time	Time Delta	Source	Destination	VLAN	Src Port	Dst Port	Protocol
239	21.047809	0.086510	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
248	21.055761	0.000498	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
364	26.993950	0.017394	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
365	26.998683	0.004733	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
600	52.303124	0.027765	fe80::21e:7aff:fe79:3f11	ff02::1	10		ICMPv6	
607	52.985973	0.058760	fe80::5:73ff:fea0:7f	ff02::1	121		ICMPv6	
849	81.047578	0.203531	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
855	81.056339	0.000511	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
937	86.995261	0.380315	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
938	86.999513	0.004252	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
1145	109.687776	0.030748	fe80::21e:7aff:fe79:3f11	ff02::1	121		ICMPv6	
1179	113.984200	0.304294	::	ff02::1:ffe9:bb47	30		ICMPv6	
1187	114.992853	0.105264	fe80::221:70ff:fee9:bb47	ff02::2	30		ICMPv6	
1220	118.781064	0.036130	fe80::221:70ff:fee9:bb47	ff02::2	30		ICMPv6	
1267	122.778808	0.003000	fe80::221:70ff:fee9:bb47	ff02::2	30		ICMPv6	
1425	141.048399	0.153152	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
1431	141.056900	0.001504	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
1512	146.996573	0.061511	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
1513	147.000321	0.003748	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
1975	195.984811	0.111397	fe80::21e:7aff:fe79:3f11	fe80::214:69ff:fe9e:1141	121		ICMPv6	
1976	195.989181	0.004370	fe80::214:69ff:fe9e:1141	fe80::21e:7aff:fe79:3f11	121		ICMPv6	
1977	195.989437	0.000256	fe80::214:69ff:fe9e:1141	2003:51:6012:121::2	121		ICMPv6	
1978	195.992932	0.003495	2003:51:6012:121::2	fe80::214:69ff:fe9e:1141	121		ICMPv6	
2020	200.929447	0.025754	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2021	201.049222	0.119775	2003:51:6012:121::2	2a01:488:42:1000:50ed:8588:8a:c570	121		ICMPv6	
2027	201.057715	0.001624	2a01:488:42:1000:50ed:8588:8a:c570	2003:51:6012:121::2	121		ICMPv6	
2031	201.069218	0.000248	fe80::214:69ff:fe9e:1141	fe80::21e:7aff:fe79:3f11	121		ICMPv6	
2032	201.072968	0.003750	fe80::21e:7aff:fe79:3f11	fe80::214:69ff:fe9e:1141	121		ICMPv6	
2072	202.033377	0.123018	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2079	203.125304	0.208297	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2097	204.933320	0.003119	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2098	205.129356	0.196036	fe80::5:73ff:fea0:7f	ff02::1	121		ICMPv6	
2111	205.965231	0.023754	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2117	206.997891	0.050376	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2136	208.937445	0.267796	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2151	210.029363	0.059761	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	
2162	211.121533	0.068257	fe80::214:69ff:fe9e:1141	ff02::1:ff00:cafe	121		ICMPv6	



IPv6 Address Assignment



- → Wireshark time... 1st pcap
- RS/RA: message 8, 12
- DAD: message 21
- DHCPv6: message 13 & 14 (recursive DNS)

- Challenge: Flags from the prefix information?
 - On-link (L), Autonomous address-configuration (A)



Link-Layer Addr. Resolution



- ARP in IPv4
- Neighbor solicitation sent to special multicast addresses ... ;(
 - 2003:50:aa10:4243:221:6aff:fe2d:3b8e
 - ff02::1:ff2d:3b8e
- Target answers with neighbor advertisement
- `icmpv6.type == 135` or `icmpv6.type == 136`



IPv6 Address Assignment



- → Wireshark time... 1st pcap
- NS: message 53 w/ link-layer option!
- NA: message 54



What's missing?



- Annoying multicast listener stuff, MLD
- Problem again: Everything is within ICMPv6
`icmpv6.type == 130 or icmpv6.type == 131 or
icmpv6.type == 132 or icmpv6.type == 143`
- Filter it out ;)
!()



To sum it up



- ICMPv6 with NDP collection
 - RS/RA 133/134
 - NS/NA 135/136
 - DAD 135 from ::
 - Ping 128/129
 - Ignoring MLD
- DHCPv6



Upper Layers stay the same



- → Wireshark time... 2nd pcap
- DNS, HTTP(S), IMAP, SMTP
- SSH, SNMP, Ping
- TL;DR: Nothing to see here

- Challenge: What's inside the HTTP answer?
 - A table (Hint: „Follow HTTP Stream“)





Network Protocols



- Protocols to manage switches & routers
- 5x link layer protocols (above Ethernet but not IP)
- 5x based on UDP
- not (dns or http or smtp)
- not (rip or ospf or bgp)
- → Wireshark time... 3rd pcap



Spanning Tree Protocol



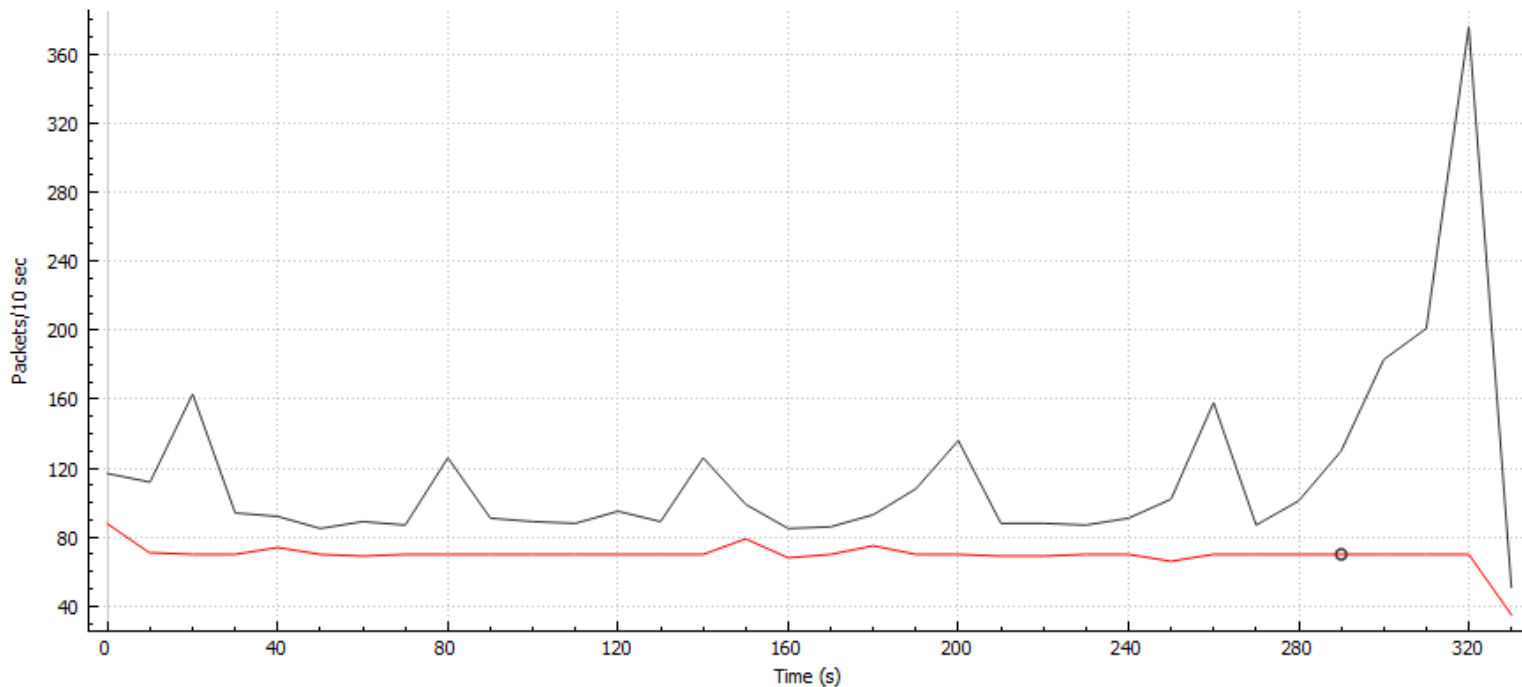
- Display Filter: `stp`
- Prevents loops within switched networks
- per VLAN, today's default: Rapid STP
- Root bridge (= switch): central point
- Hello: every 2 seconds per port per VLAN!



Spanning Tree Protocol



Wireshark IO Graphs: CCNP-SWITCH-final.pcap





Spanning Tree Protocol



- Do NOT disable it on user ports!
- Keywords: MST, BPDU, root port, designated port, port states: blocking/discarding, learning, portfast, BPDU guard, BPDU filter
- No need for STP in SDN anymore
- Challenge: Root bridge ID for VLAN 40?
 - Bridge Identifier: 24576 / 40 / 00:21:1b:ae:31:80



Cisco Discovery Protocol



- Display Filter: `cdp`
- Cisco proprietary
- Shares information about *directly connected* devices
- Keywords: TLV, CDP spoofing ;)
- Challenge: IPv4 management address of CCNP-LAB-S1?
 - 192.168.121.10



Link Layer Discovery Protocol



- Display Filter: `lldp`
- Vendor-neutral version for sharing layer 2 neighbor information
- Keywords: Information gathering ;)
- Challenge: IPv6 management address of CCNP-LAB-S1?
 - `2003:51:6012:121::10`



VLAN Trunking Protocol



- Display Filter: `vtp`
- Cisco proprietary, propagates VLAN definitions (ID & name, ...)
- Three different versions, recommended: v3, reality: v2
- Keywords: configuration revision number, VTP domain name, VTP password, VTP pruning
- Challenge: Name of VLAN 10? Hint: „ISL VLAN ID“ field is hexadecimal
 - VLAN10undsonstnix



Link Aggregation Control P.



- Display Filter: `lacp`
- Negotiates an automatic bundling of links
- aka Etherchannel, trunk, aggregated link group
- slow = 30s, fast = 1s
- Keywords: mode active/passive, system/port priority
- Challenge: seen from actor `00:0a:8a:a1:5a:80`: what's the partner port priority?
 - 32768



Hot Standby Router Protocol



- Display Filter: `hsrp`
- Cisco proprietary, redundancy of the default gateway
- Highest priority: virtual router w/ virtual IP, VIP
- Not an HA-pair of hardware, only VIPs
- Standards-based alternative: VRRP
- Keywords: HSRP group, multicast groups, virtual MAC
- Challenge: virtual IPv6 address for HSRP group 127?
 - `fe80::5:73ff:fea0:7f`



Syslog



- Display Filter: `syslog`
- Message logging to central server, e.g. SIEM, Splunk
- UDP port 514, plaintext
- TCP and TLS recommended
- Keywords: facility, severity level (0-7)
- Challenge: Which interface changed state to up?
 - Interface GigabitEthernet0/2, changed state to up



Network Time Protocol



- Display Filter: `ntp`
- Clock synchronization
- UDP port 123
- Stratum 1: synced to external source (GPS, DCF77)
- Recommended: Authentication via SHA-1
- Keywords: NTP algorithm, timestamps, SNTP, PTP
- Challenge: Reference ID from IPv6 NTP server?
 - DCFa (amplitude modulation)



Simple Network Management



- Display Filter: `snmp`
- Get/set variables from management station
- Mostly: interface and CPU/memory stats
- UDP port 161, Trap on port 162, SNMPv2c plaintext!!!
- Recommended: SNMPv3 w/ encryption & authentication
- Keywords: NMS, MIB, OID, PDU
- Challenge: What's the used community string?
 - `n5rAD1ig314IqfioYBWw`



Trivial File Transfer Protocol



- Display Filter: `tftp`
- TRIVIAL file transfer, no authentication, plaintext!!
- UDP port 69
- Common usage: config files backup
- Recommended: Don't use it at all
- Keywords: Information gathering ;)
- Challenge: Hashed password of user weberjoh?
 - `username weberjoh [...] 1kI2F$Sz18KSQV/D/QJpbpIGpH10`



(Security) Conclusion



- Use encryption/authentication!
- Avoid plaintext protocols!
- Expose your network carefully! ;D

- Take your own pcaps and have a look at them



Not covered



- PAgP, MST, DTP, UDLD, DHCP, ARP, LOOP, SSH, Telnet, RADIUS, TACACS+, EAPOL, SNMPv3, VRRP, GLBP, NetFlow, IP SLA, GRE, IKE, ESP, AH, RIP, OSPF, IS-IS, BGP, IGMP, PPP



Resources



- In general: Cisco CCNA/CCNP courses, Wikipedia, RFCs
- [IPv6 Buzz podcast "Understanding And Troubleshooting IPv6 With Wireshark"](#)
- [Wireshark Layer 2-3 pcap Analysis w/ Challenges](#)



Thx!



- Questions?
- johannes@webernetz.net

